FDSL 3.0 FIRMA DIGITAL DE SAN LUIS

MANUAL DE USUARIO SERVICIO JAVA FIRMADOR Y VALIDADOR

Servicio de Firma y Validación de Documentos Digitales FDSL



Servicio de Firma de Documentos Digitales

Antes de firmar digitalmente un documento, es necesario verificar que se cuenta con los siguientes **requisitos**:

- a) Poseer un certificado de *firma digital* vigente otorgado por el Instituto Firma Digital de San Luis.
- b) Tener instalados los drivers del dispositivo criptográfico (CIPE, Token).
- c) Tener instalada la última versión de Java.
- d) Contar con el documento a firmar en formato digital.
- e) Ejecutar la aplicación en navegador Internet Explorer 11 o Microsoft Edge

Los **pasos** que se deben seguir para firmar un documento digitalmente son:

 Ingresar al portal de Firma Digital (<u>San Luis - Firma Digital</u>) y seleccionar la opción *"FIRMAR"*



- Para navegador Microsoft Edge ver "Manual de Usuario Operativo Modo IE en Microsoft EDGE "
- La primera vez que se usa la aplicación, aparecerá un mensaje de seguridad, en el cual se debe hacer clic en la opción *"Ejecutar"*.
- Posteriormente, comenzará a cargarse la aplicación.
- 2. Una vez que se cargó la aplicación, hacer clic en el botón "Seleccionar el archivo".

Firmador

Firmador

Seleccionar Archivo Eliminar Archivo	Limpiar	
rchivos a firmar		
ra agregar firmas al documento presione "Firmar". Para finaliza	el proceso presione "Finalizar"	
ra agregar firmas al documento presione "Firmar". Para finalizat Firmar Finalizar	el proceso presione "Finalizar"	
ra agregar firmas al documento presione "Firmar". Para finaliza Firmar Finalizar	el proceso presione "Finalizar"	
ra agregar firmas al documento presione "Firmar". Para finalizar Firmar Finalizar	el proceso presione "Finalizar"	
ra agregar firmas al documento presione "Firmar". Para finalizar Firmar Finalizar	r el proceso presione "Finalizar"	
ra agregar firmas al documento presione "Firmar". Para finaliza Firmar Finalizar	el proceso presione "Finalizar"	
ra agregar firmas al documento presione "Firmar". Para finalizar Firmar Finalizar	el proceso presione "Finalizar"	
ra agregar firmas al documento presione "Firmar". Para finalizar Firmar Finalizar	el proceso presione "Finalizar"	

3. Luego, buscar el archivo a firmar en la carpeta donde el mismo fue guardado

chivos a firmar					
	Seleccion	ar			;
	Buscar en:	🕹 Descargas		v 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	• 💷 -
	Elementos	Documento de Documento de FirmaDocDigita	Prueba.docx Prueba.pdf ales.pdf		
6	Escritorio	l& ValidacionFirm	aDigital.pdf		
Firmar Final	Documentos				
	Este equipo				
_	2	Nombre de archivo:	Documento de Prueba.pdf		Seleccionar
	Red	Archivos de tipo:	Todos los Archivos	~	Cancelar

4. Al seleccionar el o los archivos que se desean firmar, los mismos aparecen listados en la aplicación de Firma.

Firmador

Seleccionar Archivo Eliminar Archivo	Limpiar
Archivos a firmar	
C:\Users\Gateway\Downloads\Documento de Prueba.docx	
C:\Users\Gateway\Downloads\Documento de Prueba.pdf	
Para agregar firmas al documento presione "Firmar". Para finaliza	r el proceso presione "Finalizar"
Firmar Finalizar	

- El o los archivos seleccionados deben encontrarse CERRADOS antes de firmarlos digitalmente
- El dispositivo criptográfico debe estar conectado a la computadora para poder firmar. Luego hacer clic en el *botón "Firmar"*.
- 5. Se despliega el panel de firma, buscar dentro de la lista de certificados que contiene el dispositivo criptográfico, el que se utilizará para firmar.

Archivos a firr	nar		
:\Users\Gate :\Users\Gate	way\Downloads\Documento de Prueba.docx way\Downloads\Documento de Prueba.pdf		-
			1
	Unitech - Firma Digital		×
	Seleccione su certificado:		
^P ara agregar fi Firmar	Lista de certificados Agencia de Ciencia Agencia de Ciencia Agencia de Ciencia Médico-exento - exesponsable de Sistemas - Oficial de Registro Central - Oficial de Registro Central - Oficial de Registro Central - Seleccione su certificado y presione sobre el b	: otón firmar	
		Firmar	Cancelar
		Firmar	Cancelar

Una vez que seleccionó el certificado pulsar el botón *"Firmar"*, la aplicación pedirá la clave de seguridad del dispositivo, colocar la contraseña.

- Una vez firmado el documento, es posible seleccionar otro certificado digital para "Firmar" el documento nuevamente
- Luego pulsar el botón "Finalizar" y se concluye la tarea saliendo de la aplicación.

Firmador

• Para asegurar que el documento quedo firmado correctamente, los mismos aparecen listados en "*Archivos firmados*".

Archivos firmados	
C:\Users\Gateway\Downloads\Documento de Prueba.docx.Luis Ala C:\Users\Gateway\Downloads\Documento de Prueba.ndf	iniz.pki
n loon o loane way loomini dab loorannen to de in acoalpar	
	Firmar más archivo
ramix PKI - Servicios - Versión 12.14.0	firma

• Para iniciar una nueva tarea pulsar "Firmar más archivos"

IMPORTANTE:

- En caso de que el certificado seleccionado esté revocado, no se podrá firmar el documento y se mostrará el mensaje "El certificado con el que se intenta firmar está revocado". Del mismo modo, si el certificado con el que se intenta firmar está vencido se mostrará un mensaje "El certificado con el que se intenta firmar ha caducado".
- Para los documentos que no son en formato .pdf, el o los archivos "digesto" generados luego de firmar el documento (con extensión .pki) son guardados en la misma carpeta en la que se encuentra el archivo original, con el mismo nombre del documento + nombre del firmante.

Hoy (2)
Documento de Prueba.docx.Luis Alaniz.pki
Documento de Prueba.docx

• En el caso que se firme un archivo en formato .pdf, la firma queda incrustada dentro del mismo archivo, se puede visualizar desde el "Panel de Firma" y NO se genera un "digesto" con extensión .pki.



Servicio de Validación de Documentos Digitales

Antes de validar un documento firmado digitalmente, es necesario verificar que se cuenta con los siguientes **requisitos**:

- a) Tener instalada la última versión de Java.
- b) Contar con un documento firmado digitalmente.
- c) Ejecutar la aplicación en navegador Internet Explorer 11 o Microsoft Edge
- d) Para los casos en que el archivo NO es en formato .pdf, se debe tener el digesto firmado (archivo .pki) guardado en la misma carpeta que el documento original

Los **pasos** que se deben seguir para validar un documento firmado digitalmente son:

 Ingresar al portal de Firma Digital (<u>San Luis - Firma Digital</u>) y seleccionar la opción "VALIDAR" (



- Para navegador Microsoft Edge ver "Manual de Usuario Operativo Modo IE en Microsoft EDGE "
- La primera vez que se usa la aplicación, aparecerá un mensaje de seguridad, en el cual se debe hacer clic en la opción *"Ejecutar"*.
- Posteriormente, comenzará a cargarse la aplicación.
- 2. Una vez que se cargó la aplicación, hacer clic en el botón "Seleccionar Archivo".

Validador

	Eliminar digesto	
rchivos		
		Validar y firmar Valida

3. Luego, buscar el archivo firmado en la carpeta donde el mismo fue guardado.

Seleccion	ar			×
Buscar en:	🕹 Descargas		 Ø I 	≫
lementos	Documento de Documento de Albania de Documento de	Prueba.docx Prueba.docx.Luis Alaniz.pki <mark>Prueba.pdf</mark>		
Escritorio				
Documentos				
Este equipo				
2	Nombre de archivo:	Documento de Prueba.pdf		Seleccionar
Red	Archivos de tipo:	Todos los Archivos	~	Cancelar

Validador

• Al seleccionar el archivo, el mismo aparecerá en la aplicación de validación de firma.

• Para los casos en que los archivos no son en formato .pdf, el digesto (archivo .pki) se incorporará automáticamente en la aplicación. Si el archivo a validar, no tiene el archivo digesto guardado en la misma carpeta, el mismo deberá ser buscado manualmente.

Validador

ocumento de Prueba.docx		
Agregar el digesto firmado	Eliminar digesto	
Archivos		
:\Users\Gateway\Downloads\Docume	ento de Prueba.docx.Luis Alaniz.pki	

• En el caso de querer validar un archivo en formato .pdf, NO es necesario agregar un digesto (archivo .pki), porque el mismo contiene la firma incrustada en el archivo original.

ocumento de Prueba.pdf			
Agregar el digesto firmado	Eliminar digesto		
rchivos			

- 4. Luego hacer click en el botón "VALIDAR"
- Al momento de hacer la validación, si el documento original y/o su archivo digesto no sufrieron modificaciones, se muestra una ventana indicando que "La firma es válida".
- En caso de que la firma no es válida, ya sea porque se modificó el documento original o porque el archivo de firma no es el correcto, se muestra una ventana indicando que "La firma no es válida".
- Seleccionando "validar más archivos" se pueden agregar más archivos para validar.

Documento de Prueba.p Resultado de la validación	tf 1 de firmas:		
Firmante	Resultado	Estado del certificado	
Luis Alaniz	🖌 La firma es válida	Vigente	
Validador			
Validador Archivo validado Documento de Prueba.d	ocx		
Validador Archivo validado Documento de Prueba.d Resultado de la validació	ocx n de firmas:		
Validador Archivo validado Documento de Prueba.d Resultado de la validació Firmante	ocx n de firmas: Resultado	Estado del certificado	

Validador

- El icono 0 permite ver información del certificado digital que firmó el documento.

Validador

rmante		Resultado	Estado del e	certificado	
is Alaniz		🎸 La firma es válida	Vigente		0
🗔 Certificado				×	
🖌 l a firma e	c bilèv a				
	s valiua.				
General Detalles					
Información d	el certificado				
Este certificado esta	a destinado a	los siguientes propósitos	:		
[1.3.6.1.5.5.7.3.	2, 1.3.6.1.4.1	.311.20.2.2, 1.3.6.1.5.5.7	.3.4, 2.16.32.1.3.2	.1.1.1]	
– Enviado a:	Luis Alaniz				
Emitido por p	RUEBA FDSL	- AC Agentes del Estado		fir	masarchivos
Válido desde	15/03/2022	2 15:08 hasta 15/03/2	026 15:08	d	gital

• En la *solapa "Detalles"* se muestran los datos del certificado digital con el cual se firmó el documento.

esultado de la validación de	firmas:			
rmante	Resultado	Estado del cert	tificado	
is Alaniz	🖌 La firma es válida	Vigente		
V La firma es v	válida.			
Campo	Valor			
Versión	3			
Número de serie	1a 00 00 01 43 0	53 d7 e3 64 31 29 b9		
Algoritmo de firma	sha256RSAENCR	(YPTION		
Emisor	C=AR,ST=San L	uis,SERIALNUMBER=		
		18		
Válido desde	15/03/2022 13:0	18		
Vàlido desde Valido hasta Asunto	15/03/2022 15:0 15/03/2026 15:0 C=AB ST=SAN)8 UIS E=lalaniz@uln.ed		
Válido desde Valido hasta Asunto Clave pública	15/03/2022 15:0 15/03/2026 15:0 C=AR,ST=SAN I 30 82 01 22 30 0	08 UIS,E=lalaniz@ulp.ed 0d 06 09 2a 86 48 86		
Valido desde Valido hasta Asunto Clave pública Identificador de clave en	15/03/2022 15:0 15/03/2026 15:0 C=AR,ST=SAN I 30 82 01 22 30 0 11/24 emisora f7 03 3d 8c 06 fe	08 .UIS,E=lalaniz@ulp.ed 0d 06 09 2a 86 48 86 1 5e fd 3a e1 ea c0 bd		
Valido desde Valido hasta Asunto Clave pública Identificador de clave en C=AR	15/03/2022 15:0 15/03/2026 15:0 C=AR,ST=SAN 30 82 01 22 30 (11/2 03 3d 8c 06 fd	8 UIS,E=lalaniz@ulp.ed 0d 06 09 2a 86 48 86 1 5e fd 3a e1 ea c9 bd		
Valido desde Valido hasta Asunto Clave pública Identificador de clave er C=AR ST=SAN LUIS	15/03/2022 15:0 15/03/2026 15:0 C=AR,ST=SAN 1 30 82 01 22 30 0 31 de misora f7 03 3d 8c 06 f4	8 UIS,E=lalaniz@ulp.ed 0d 06 09 2a 86 48 86 1 56 fd 3a e1 ea c0 bd		
Valido desde Valido hasta Asunto Clave pública Identificador de clave er C=AR ST=SAN LUIS E=lalaniz@ulp.edu	13/03/2022 13:0 15/03/2026 13:0 C=AR,ST=SAH 30 82 01 22 30 0 tidad emisora f2 03 3d 8c 06 fe	8 .UIS,E=lalaniz@ulp.ed od 06 09 2a 86 48 86 I Se fd 3a e1 ea c0 bd	Validat	r más archivos
Valido desde Valido hasta Asunto Clave pública Udantificador de clave ar C=AR ST=SAN LUIS E=lalaniz@ulp.edu T=Responsable de	13/03/2022 15: 15/03/2022 15: C=AR_ST=5AH 30 82 01 22 31 0 30 82 01 22 31 0 31 42 06 fe .ar Sistemas	8 UIS,E= alaniz@ulp.ed)d 06 09 2a 86 48 86 I 56 fd 3a e1 ea c0 bd	Validar	r más archivos
Valido hesde Valido hesda Asunto Clave pública Lidantificador.de.clave.er C=AR ST=SAN LUIS E=Lalaniz@ulp.edu T=Responsable de OU=Instituto Firm	13/03/2022 15: 15/03/2022 15: C=AR_ST=SAN 30 82 01 22 30 0 abidad amisora f7.03.3d Br. 06 f6 .ar Sistemas a Digital de San Luis	8 UJS,E=lalaniz@ulp.ed. UJS,E=lalaniz@ulp.ed. 0 06 09 2a 86 48 86 1 5e fd 3a e1 ea c9 bd	Valida	r más archivos
Valido hesde Valido hesda Gave pública Identificador da clave er C=AR ST=SAN LUIS E=lalaniz@ulp.edu T=Responsable de 00=Instituto Firm 0=Agencia de Cien	.ar Sistemas a Digital de San Luis cita Tecnología y Socied	8 UIS.E=lalaniz@ulp.ed. 0d 06 09 2a 86 48 86 5 5 fd 3a al aa c0 bd	Valida	r más archivos
Valido hesde Valido hesda Asunto Clave pública Lidantificador.da.clave.ar C=AR ST=SAN LUIS E=lalaniz@ulp.edu T=Responsable de 00=Instituto Firm 0=Agencia de Cien SERIALNUMER=CULL	IJU034022 15: IJU032026 15: C=AR_ST=5AN algorithm of the second secon	8 UIS,E=Balaniz@ulp.ed., 0 60 99 2a 86 48 86 1 5a fd 3a al az c0 hd_ ad San Luis	Validar	más archivos

IMPORTANTE:

El proceso de validez de firma, Consiste en aplicar al documento original el algoritmo Hash, y por otro lado descifra el archivo firmado con la clave pública del firmante que está contenida en el digesto (archivo .pki). Luego se comparan ambos resultados y si coinciden se deduce que la firma es válida, caso contrario no se debe confiar en la integridad del documento original.